MULTIMEDIA UNIVERSITY®

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2018/2019

ECE3246 – SECURITY & CRYPTOGRAPHY

(CE, TE, ME)

11 MARCH 2019
2.30 – 4.30 pm
(2 Hours)

INSTRUCTIONS TO STUDENT

1. This examination paper consists of 6 pages including the cover page with 4 questions only.
2. Attempt **any THREE** out of **FOUR** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

Question 1

a) Describe your understanding of the following *security concepts*:

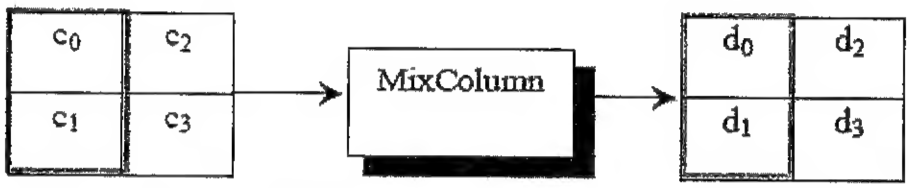
(i) *cipher mode of operation* [3 marks]

(ii) *one-wayness* [3 marks]

b) (i) Discuss the reasons why a *block cipher* and a *message authentication code* (MAC) are **not** considered as *public-key cryptography* (PKC) techniques. [3 marks]

(ii) Discuss the reasons why all *round functions* of a *block cipher* need to be keyed by a *round key*. [3 marks]

c)



where $\begin{bmatrix} d_0 \\ d_1 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$ and $\begin{bmatrix} d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} c_2 \\ c_3 \end{bmatrix}$

Figure 1 MixColumns operation of Mini-AES

Recall the *MixColumn* (MC) and *AddRoundkey* (AR) operations of Mini-AES. MC is performed as per Figure 1, i.e. each column of the input matrix is taken as a column vector to be matrix multiplied with a constant matrix (3,2;2,3).

Firstly, when one input (c_0,c_1,c_2,c_3) is processed by *MixColumn*, its output denoted by (d_0,d_1,d_2,d_3) is produced.

***Question*:** Secondly, if a slightly different input (x_0,c_1,c_2,c_3) is put through *MixColumn* to get the output (y_0,y_1,y_2,y_3), i.e. only the first element x_0 of the second input is different from c_0 of the first input, while the others c_1,c_2,c_3 remain the same; discuss which elements of the second output (y_0,y_1,y_2,y_3) will be **different** from the first output (d_0,d_1,d_2,d_3) and why. [8 marks]

Continued...

Question 2

a) *Biometrics* is a type of '**what you are**' factor used for authentication. In comparison with the '**what you know**' factor for authentication, discuss which type is easier/harder to be *accessed/known* by the attacker, as well as which type is easier/harder to be *forged/reproduced* by the attacker. [3+3 marks]

b) A hash function *h*( ) is typically applied to an input message *m* before it is signed by a digital signature function *Sign*( ), i.e. the signature output *sig* = *Sign*(*h*(*m*)). Given two different input messages *m1* and *m2*, leading to outputs *sig1* and *sig2*, discuss using these symbols, why it is important for the hash function *h*( ) to have the property of **collision-resistance**.

[6 marks]

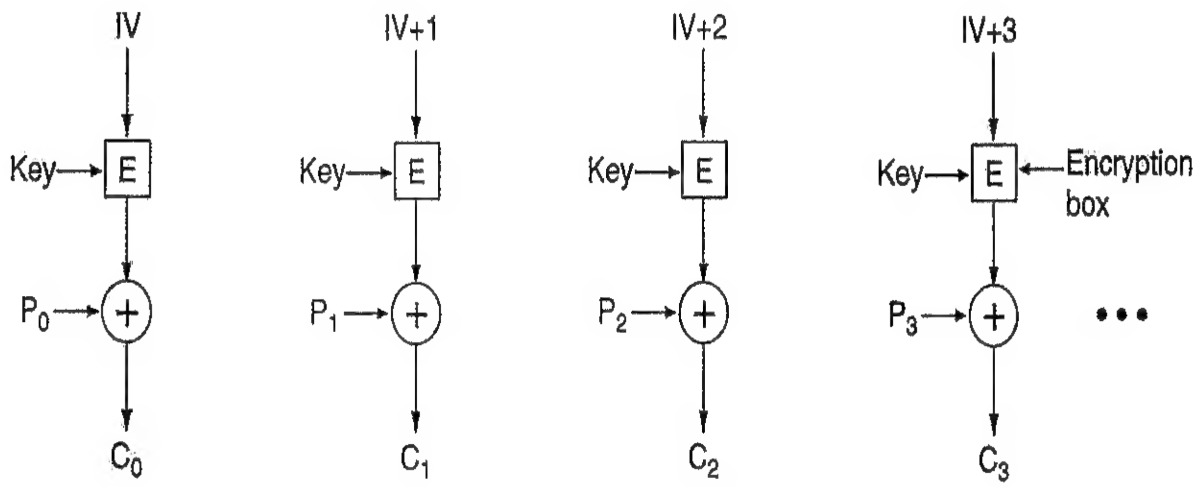


Figure 2 [sourced from http://homepage.smc.edu/morgan_david/linsec]

c) Figure 2 illustrates an *operation mode* for a *block cipher E*.

(i) Discuss whether this operation is **invertible** or not. [4 marks]

(ii) Discuss what happens at the receiver side when an attacker has mounted a *replacement attack* to replace block C0 while the other blocks remain unchanged. [4 marks]

Continued...

Question 3

a) (i) Describe the basic idea behind the **deterministic problem** exhibited by *textbook RSA*. [3 marks]

(ii) Describe how *public key cryptography* could solve the **key distribution problem.** [3 marks]

b) The *RSA public key cipher* performs encryption defined as follows

$c = m^e \bmod n$

where c is the ciphertext, m the plaintext, e the public key and n the modulus, and decryption is defined as

$m = c^d \bmod n.$

Given that the public key e is 7, private key d is 23, and modulus n is 55; show how a plaintext $m = 8$ can be *encrypted.* [6 marks]

c) A *homomorphic encryption* scheme $E(\ )$ is said to satisfy the following type of property:

$$E(m1) \,.\, \mathrm{E}(m2) = E(m1.m2)$$ for some operation denoted by .

The encryption function of the **Paillier** encryption scheme is given as follows, where g and n are public parameters, and r is an ephemeral random number which differs each time the encryption function is called:

$$c = g^m \cdot r^n \bmod n^2$$

Show by using appropriate example symbols e.g. $m1$, $m2$, ... $c1$, $c2$, ... why Paillier has the **homomorphic property**.

[8 marks]

Continued...

Question 4

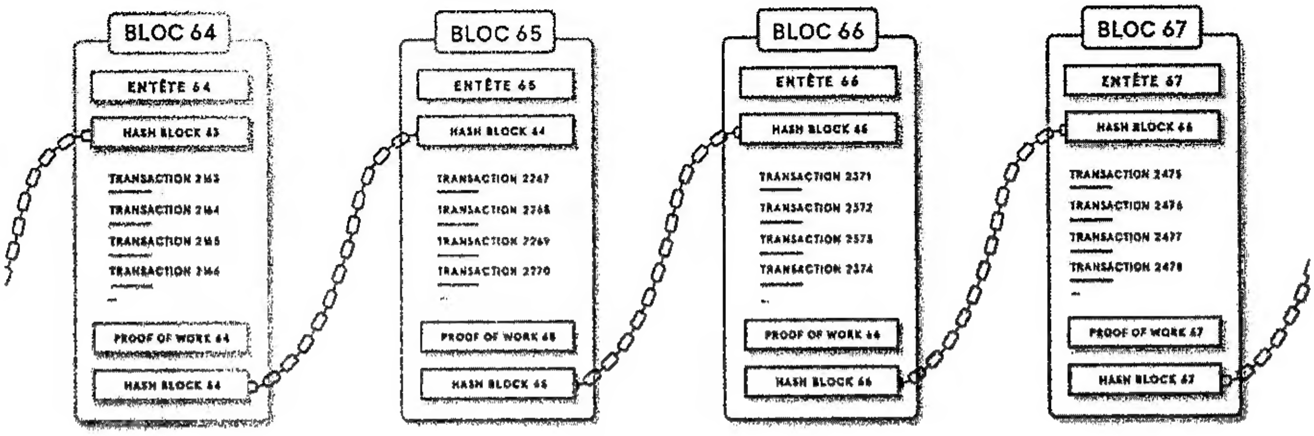


Figure 3 [sourced from https://blog.theodo.fr]

a) Figure 3 shows the sketch of a *block chain.*

(i) Describe your understanding of what is a block chain. [3 marks]

(ii) What cryptographic functions are used in a block chain? Explain. [3 marks]

b)

(i) Discuss your understanding of the concept of *anomaly detection* and how that relates to *network security*. [3 marks]

(ii) Describe your understanding of the concept of *computations in the encrypted domain* and how that relates to *cloud security*. [3 marks]

Continued...

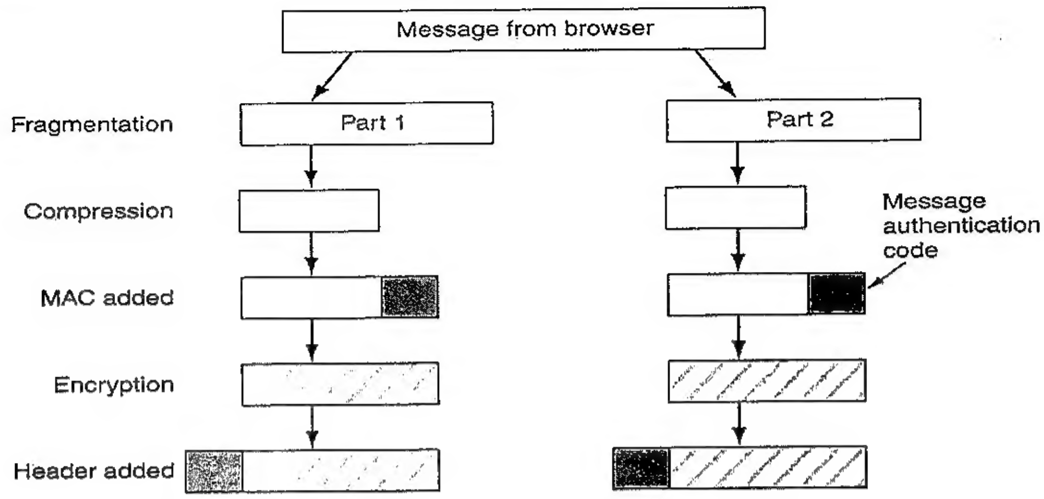


Figure 4

c)

Figure 4 shows the *Transport Sub-protocol* of the Secure Sockets Layer (SSL), in particular the operations performed at the sender side. More precisely, for fragment m1, the following is computed and sent to the recipient:

z = header || Encrypt (Compress(m1) || MAC(m1))

(i) Note that MAC is performed before Encryption; this approach is so-called *authenticate-then-encrypt* (AtE). Describe your understanding of how this works at the **transmitting side.** [4 marks]

(ii) Consequently, discuss what happens at the **receiving side** for this approach of authenticate-then-encrypt (AtE).

[4 marks]

End of Paper